



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/643,101	08/18/2003	Michael Arnouse	1232-R-03	3339

35811 7590 09/22/2004

IP DEPARTMENT OF PIPER RUDNICK LLP  
ONE LIBERTY PLACE, SUITE 4900  
1650 MARKET ST  
PHILADELPHIA, PA 19103

EXAMINER

AHMED, SAMIR ANWAR

ART UNIT PAPER NUMBER

2623

DATE MAILED: 09/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 10/643,101	<b>Applicant(s)</b> ARNOUSE, MICHAEL	
	<b>Examiner</b> Samir A. Ahmed	<b>Art Unit</b> 2623	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
  - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
  - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
  - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-58 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-58 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>8/18/03</u> . | 6) <input type="checkbox"/> Other: ____.  |

### DETAILED ACTION

1. The amendment filed 6/24/04 is objected to under 35 U.S.C. 132 because it introduces new matter into the disclosure. 35 U.S.C. 132 states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: the original embodiment of controlling an aircraft is disclosed using a "rudder controller" of the aircraft as recited in the originally filed specification, the provisional application 60/482807 that this application claims priority to and the originally filed drawings, removing "rudder" from the specification and the drawings is broadening the scope and is equivalent to introducing new subject matter of controlling the aircraft using any controller and no specific controller.

Applicant is required to cancel the new matter in the reply to this Office Action.

2. The subject matter disclosed in claims 6-11, 13-16, 18, 22-23, 27-29, 31-33, 35-37, 40, 45, 48-49, 53-54, 56-58 is denied priority to provisional 60/482807 and have the filing date of this application (8/18/03) because it is not recited anywhere in the provisional application. For example "comparing of the user characteristic against biometric information stored in the one computer" recited in claim 6, is not found anywhere in the provisional.

### ***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the

Art Unit: 2623

art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 26, 39, 52 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Claim 26, recites "engaging or disengaging the auto pilot where it is determined that an authorized person is in the pilot or copilot seat". This feature is not enabled by the specification because as shown in Fig. 4, at step 228 when it determined an authorized pilot in seat, the system allows disengagement of auto pilot (not engaging or disengaging).

As to claims 39, 52, refer to claim 26 rejection.

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 13 and 46 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 13 recites the limitation "the control" in line 2. There is insufficient antecedent basis for this limitation in the claim.

As to claim 46 refer to claim 13 rejection.

***Claim Rejections - 35 USC § 102***

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-5, are rejected under 35 U.S.C. 102(e) as being anticipated by Seah et al. (U.S. Patent Application Publication 2003/0071743).

As to claim 1, Seah discloses a security mechanism for identifying authorized users comprising:

a controller operable by a user [cockpit double door module or autopilot subsystem or communication systems (controller) used by user (i.e. operable by a user) (col. 3, [0050])];

one or more security devices to identify the user attempting to operate the controller [fingerprint devices, retina scanners (security devices) to identify the user trying to gain access to the controller (col. 3, [0050])]; and

one or more monitoring devices to determine whether the user identified is authorized to operate the controller [on-board computer system (monitoring device) (Fig. 2, item 36) to determine whether the user is authorized to gain access or not (col. 3, [0050])].

As to claim 2, Seah further discloses, wherein the one or more security

devices comprise at least one biometric device [col. 2, 0045].

As to claim 3, Seah further discloses, a fingerprint/pulse reader on the controller [biometric devices are integrated into the cockpit double door module or autopilot subsystem and includes fingerprint reader (i.e. on the controller) [col. 3, 0050].

As to claim 4, Seah further discloses, wherein the at least one biometric device further comprises a retina reader on the controller [biometric devices are integrated into the cockpit double door module or autopilot subsystem and includes retina scanner (i.e. on the controller) [col. 3, 0050].

As to claim 5, Seah further discloses, wherein the controller comprises a control of an aircraft [autopilot module is a controller that controls an aircraft (col. 3, 0050)].

9. Claims 8-9, 12-18, 20-22, 27-31, 33-35, 40-41, 44-48, 53, 58 are rejected under 35 U.S.C. 102(e) as being anticipated by Riley (U.S. Patent Application Publication 2003/0067379).

As to claim 8, Riley discloses a security system for restricting operation of an aircraft comprising:

one or more biometric devices for reading biometric information of a person attempting to operate the aircraft [scanning means such as fingerprint scanning device 7, or devices, mounted on the primary aircraft controls or any other suitable location on the cockpit (col. 3, [0038])];

one or more monitoring systems in communication with the one or more biometric devices, the one or more monitoring systems comparing the biometric information read by the one or more biometric devices against stored biometric

information concerning authorized persons to operate the aircraft [microprocessor module 2 (monitoring system in communication with biometric devices) receives the fingerprint image from the fingerprint scanning device 7 (col. 3, [0038]), the microprocessor control module 2 compares the user's fingerprint received from the biometric scanner 7 with a stored fingerprint template to authenticate the user (col. 4, [0042])); and

one or more control mechanisms in communication with the one or more monitoring systems to regulate operation of the aircraft based on whether or not an authorized person has been identified [a communication module 3 (control mechanism) is connected to (in communication with) the microprocessor 2 and connected to transponder or autopilot (control mechanisms) (col. 5, [0048]), the operation of such control mechanisms is regulated based on the verification result (col. 2, [0023], col. 5, [0050])).

As to claim 9, Riley further discloses, wherein the one or more biometric devices comprises a fingerprint reader on at least one of a control of the aircraft [col. 5, [0048], Figs 1, 2 and 3], an access door to the cockpit area, or an access door to a storage compartment.

As to claim 12, Riley further discloses, wherein the one or more monitoring systems comprises at least one computer [Fig. 1, microprocessor 2] and the one or more biometric devices comprises at least one of a fingerprint reader [fig. 1, fingerprint reader 7], a pulse reader or a retina reader.

Art Unit: 2623

As to claim 13, Riley further discloses, wherein the one or more control mechanisms comprises at least one of the auto pilot control system (col. 2, [0014]), the control [Fig 1, item 11, Fig.2, item 7, Fig. 3, item12, (col. 5, [0048])], aircraft beacon system [aircraft transponder (beacon) (col. 4, [0043])], a GPS system (col. 4, [0041]) or any system controlled by the control.

As to claim 14, Riley discloses a method for regulating operation of an aircraft comprising:

storing biometric information electronically regarding persons of a designated flight authorized to operate the aircraft [authorized flight personnel having their fingerprint images (biometric information) stored in smart card memory (electronic storage) (col. 4, [0046]);

reading biometric information from any person attempting to operate the aircraft (col. 5, [0048]);

comparing the read biometric information against the stored biometric information to aircraft is authorized to operate the determine whether the person attempting to operate the aircraft (col. 5, [0050]); and

allowing authorized persons to operate the aircraft [when the fingerprint matches the stored fingerprint, the identity of the person operating the aircraft controls is authenticated (col. 5, [0050]) and the user is allowed to operate the aircraft col. [0013]].

As to claim 15, Riley further discloses, comprising performing a biometric check of persons authorized to operate the aircraft prior to flight (col. 1, [0013]).



As to claim 16, Riley further discloses, wherein operating comprises at least one of flying the aircraft [providing in-flight aircraft flight crew authentication (i.e., flying the aircraft) (col. 1, [0013])], opening an access door to the cockpit area, or opening an access door to a storage compartment.

As to claim 17, Riley further discloses, wherein attempting to fly the aircraft comprises grasping of a control [Fig. 1, shows fingerprint device 7 located on the control yoke 11 of an aircraft and a crew member trying to fly the aircraft have to grasp that control yoke in order to fly the aircraft].

As to claim 18, Riley further discloses, wherein reading biometric information comprises at least one of reading fingerprints, pulses or retina of the person attempting to fly the aircraft when the person is grasping the control [Fig. 1, shows fingerprint device 7 (biometric information reader) located on the control yoke 11 of an aircraft and a crew member trying to fly the aircraft have to grasp that control yoke in order to fly the aircraft] or attempting to open an access door to the cockpit area or storage compartment.

As to claim 20, Riley further discloses, further comprising restricting function of the control if it is determined that the person is not authorized to fly the aircraft [upon failure to authenticate identity of the person at the controls of the aircraft, a signal is sent to the autopilot system to instruct it to fly a safe flight pattern and to disable the manual flight controls (restrict function of control) (col. 2, [0023], col. 5, [0050])].

As to claim 21, Riley further discloses, further comprising operating the aircraft in auto pilot mode when an unauthorized person attempts to fly the aircraft (col. 2, [0023], col. 5, [0050]).

As to claim 22, Riley further discloses, further comprising alerting authorities outside of the aircraft when an unauthorized person attempts to fly the aircraft (col. 2, [0022], col. 5, [0050]).

As to claim 27 refer to claim 14 rejection.

As to claim 28 refer to claim 15 rejection.

As to claim 29 refer to claim 16 rejection.

As to claim 30 refer to claim 17 rejection.

As to claim 31 refer to claim 18 rejection.

As to claim 33 refer to claim 20 rejection.

As to claim 34 refer to claim 21 rejection.

As to claim 35 refer to claim 22 rejection.

As to claim 40 refer to claim 8 rejection. Riley further discloses an aircraft comprising a controller operable to fly the aircraft [Fig. 1, shows the control yoke 11 of an aircraft used to fly the aircraft].

As to claim 41 refer to claim 9 rejection.

As to claim 44 refer to claim 12 rejection.

As to claim 45 refer to claim 13 rejection.

As to claim 46 refer to claim 20 rejection.

As to claim 47 refer to claim 21 rejection.

As to claim 48 refer to claim 22 rejection.

As to claim 53, Riley further discloses, further comprising a GPS system in communication with the one or more monitoring systems for sending position information to designated locations when at least one of an unauthorized person is identified [when an unauthorized person is identified at the controls of the aircraft, a signal or message is communicated to an appropriate outside parties (designated locations) (col. 2, [0022]). The predetermined message or signal is sent to parties outside the aircraft such as air traffic control tower (designated locations) from the aircraft's onboard transponder and/or communication system 3 in communication with the microprocessor control module 2 (monitoring system), the communication system 3 includes a GPS system and relay the positional data provided by the GPS in the predetermined emergency signal (col. 3, [0041])] or the aircraft flies off its normal course.

As to claim 58, Riley further discloses, further comprising an aircraft beacon system in communication with the one or more monitoring systems, wherein an unauthorized person is unable to turn off the aircraft beacon system [when an unauthorized person is identified at the controls of the aircraft, a signal or message is communicated to an appropriate outside parties (col. 2, [0022]). The predetermined message or signal is sent to parties outside the aircraft such as air traffic control tower from the aircraft's onboard transponder (beacon) and/or communication system 3 in communication with the microprocessor control module 2 (monitoring system) (col. 3, [0041]). The onboard communications device, such as a transponder communicates

with parties outside the aircraft with radio frequency (i.e., the transponder is a RF transmitter which reads on beacon), the transponder is always active (i.e., cannot be turn off) (col. 4, [0043]).

***Claim Rejections - 35 USC § 103***

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Seah et al. (U.S. Patent Application Publication 2003/0071743) as applied to claim 1 above, and further in view of Gehlot (U.S. Patent 6,167,333).

As to claim 6, Seah discloses a biometric subsystem such as fingerprint and retina devices in communication with the onboard computer (monitoring device) to identify and authenticate a person trying to gain access to part of the airplane or control systems such as autopilot as being authorized or not (col. 2, [0045], col. 3, [0050]) without disclosing the details of the identification or authentication process. Seah does not specifically disclose, wherein the one or more monitoring devices comprises at least one computer and the one or more security devices comprises at least one biometric device, with the at least one biometric device reading a characteristic of the user that is compared against biometric information stored in the at least one computer. However identifying a user by comparing a characteristic of the user (fingerprint or retina scan)

Art Unit: 2623

against biometric information stored in the computer is conventional and well known in the art as disclosed by Gehlot. Gehlot discloses a system for preventing an unauthorized access to a vehicle, plane (airplane) and the like (col. 3, lines 38-51). The system comprises a vehicle data processor (VDP) that compares received physical data of the user such as fingerprint or retina scan with previously stored physical data to determine whether the user is authorized (col. 2, lines 9-11, col. 3, lines 18-32, col. 5, line 63-col. 6, line 6). It would have been obvious to one having ordinary skill in the art at the time the invention was made to use the teachings of Gehlot to modify Seah's mechanism, by comparing received physical data of the user such as fingerprint or retina scan with previously stored physical data to determine whether the user is authorized and deter unauthorized use of a vehicle and prevent theft or hijacking of the vehicle.

As to claim 7, both Seah [autopilot subsystem, communications system (one or more control mechanisms in communication with the onboard computer, controls access to the autopilot module and communication system based on whether or not the user is authorized (col. 3, [0050] and [0051])) and Geholt [Fig. 1, ignition system, fuel flow system, transmission system (one or more control mechanisms) in communication with the VDP, controls access to these control mechanisms based on whether or not the user is authorized] further discloses, further comprising one or more control mechanisms in communication with the one or more monitoring devices, with the one or more monitoring devices regulating the one or more control mechanisms to restrict operation based on whether or not the user is authorized to operate the controller.

12. Claims 10-11, 19, 32 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Riley (U.S. Patent Application Publication 2003/0067379) as applied to claims 8, 14 and 27 above, and further in view of Osten et al. (U.S. Patent 5,719,950).

As to claim 10, Riley discloses the use of a fingerprint scanner (biometric device) that has live finger detection capabilities to add a further measure of security (col. 3, [0039], last nine lines), the fingerprint scanner is mounted on the aircraft's control yoke 11 (control of aircraft) (Fig. 1, Yoke 11, fingerprint scanner 7). Riley does disclose the specifics of the fingerprint scanner (biometric device) that has live finger detection capabilities and is silent about, wherein the one or more biometric devices comprises a pulse reader on at least one of a control of the aircraft, an access door to the cockpit area, or an access door to a storage compartment. However, using a pulse reader with the fingerprint scanner (biometric device) to detect a live finger in the context of access control is conventional and well known in the art as disclosed by Osten.

Osten discloses a biometric system to assure that an individual seeking biometric authentication, recognition or access is actually present for authentication. For example, in a fingerprint scanner whether the finger is attached to a living human being or an electronic or photographic reconstruction of the fingerprint or dismemberment of the finger is used (col. 1, line 56-col. 2, line 10). One or more non-specific biometric parameters (e.g., bone structure, EKG signals, pulse, and spectral characteristics of human tissue (col. 2, line 66-col. 3, line 13) used in combination with one or more unique, inherently specific biometric parameters (e.g., fingerprints, handwriting and

Art Unit: 2623

retinal configuration) (col. 2, lines 54-65) provides extremely high precision protection against circumvention, and does not require time consuming and inordinate measurement for authentication for purposes such as access control to a secure function or fitness to perform a function (col. 3, lines 14-20). Inherently specific and non-specific biometric parameters can be concurrently and non-invasively gathered for recognition, comparison, and authentication (col. 4, lines 43-46). It would have been obvious to one having ordinary skill in the art at the time the invention was made to use the teachings of Osten to modify Riley's security system by using a pulse reader in the fingerprint scanner to achieve a live finger detection capabilities (as disclosed by Riley) and concurrently gathering inherently specific (fingerprint, and retinal configuration) and non-specific (EKG signals, pulse, and spectral characteristics of human tissue) biometric parameters (as disclosed by Osten) in order to add a further measure of security and to provide extremely high precision protection against circumvention, and does not require time consuming and inordinate measurement for authentication for purposes such as access control to a secure function or fitness to perform a function.

As to claim 11, Osten further discloses, wherein the one or more biometric devices comprises a retina reader mounted in the cockpit area or on the control of the aircraft [multiple biometric parameters are used for individuals seeking authentication with security measures that potentially avoid false authentication (col. 4, lines 50-53), biometric parameters are fingerprints, signature and retinal configuration (col. 2, lines 54-65).

As to claim 19, refer to claim 10 and 11 rejections. Riley further discloses, as shown in Fig. 1, a biometric information reader (fingerprint device 7) located on the control yoke 11 (control) of an aircraft and a crew member trying to fly the aircraft have to grasp that control yoke in order to fly the aircraft, i.e. the biometric information is read when the person is grasping the control.

As to claim 32, refer to claim 19 rejection.

As to claim 42, refer to claim 10 rejection.

13. Claims 23, 25-26, 36, 38-39, 49, 51-52, 54-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Riley (U.S. Patent Application Publication 2003/0067379) as applied to claims 14, 27 and 40 above, and further in view of Seah et al. (U.S. Patent Application Publication 2003/0071743).

As to claim 23, Riley further discloses sending a predetermined signal and /or message to parties outside the airplane such as air traffic control tower upon detection of an unauthorized person (col. 3, [0041], col. 5, [0050]). Riley does specifically disclose sending of at least one of biometric information or photograph read from an unauthorized person to authorities outside of the aircraft.

Seah discloses a monitoring and incident management system for an aircraft. A monitoring device 50, such as a video camera is preferably located within the cockpit doorframe to enable crewmembers and the ground center 14 to observe any one entering the door module (col. 2, [0045]). A surveillance and sensor subsystem 24 comprises a variety of devices (such as a video camera) to detect potential threats to the safety of the aircraft and enable the ground center to monitor activities inside the



aircraft (col.3, [0052]). Compressed video images (photograph of unauthorized person) transmitted to the ground station (authorities outside the aircraft), so that ground troops waiting at a forward command post can have access to the video data captured by the video module before storming the aircraft (col. 3, [0057]). It would have been obvious to one having ordinary skill in the art at the time the invention was made to use the teachings of Seah to modify Riley's security system by transmitting video images of a persons entered unauthorized portions of the aircraft (photograph of unauthorized person) to the ground station (authorities outside the aircraft, in order to ground troops waiting at a forward command post can have access to the video data captured by the video module before storming the aircraft.

As to claim 36, refer to claim 23 rejection.

As to claim 49, refer to claim 23 rejection.

As to claim 25, Riley further discloses, as shown in Fig. 1, a biometric information reader (fingerprint device 7) located on the control yoke 11 (control) of an aircraft, which is normally controlled by a person flying the aircraft and is seated in the pilot or copilot seat. Riley does not specifically disclose, wherein reading biometric information comprises a retina read of the person attempting to fly the aircraft when the person is seated in either a pilot or copilot seat.

Seah discloses a monitoring and incident management system for an aircraft. A biometric device, such as a fingerprint or retinal scanner is provided (col. 2, [0045]). The biometric subsystem is integrated into the autopilot subsystem or the communications system, to determine whether a person trying to gain access to these

controls is authorized (col. 3, [0050]). As shown in Fig. 10, the main instrument panel 74 is located in front of the pilot and copilot seats 78, 80 and the control stand 76 is positioned between the two seats 78 and 80. The autopilot subsystem or the communications system are normally located on the main instrument panel 74 and control stand 76, i.e. proximate to the pilot and copilot seats. The biometrics subsystem will prevent a hijacker or terrorist at the pilot seat from controlling the aircraft 12 (col. 6, [00123]). It would have been obvious to one having ordinary skill in the art at the time the invention was made to use the teachings of Seah to modify Riley's security system by using a retina reader to determine whether a person at the pilot seat is authorized in order to prevent a hijacker or terrorist at the pilot seat from controlling the aircraft.

As to claim 26, both Riley (col. 5, 0050]) and Seah (col. 3, [0051] further disclose, further comprising engaging or disengaging the auto pilot where it is determined that an authorized person is in the pilot or copilot seat.

As to claim 38, refer to claim 25 rejection.

As to claim 39, refer to claim 26 rejection.

As to claim 51, refer to claim 25 rejection.

As to claim 52, refer to claim 26 rejection.

As to claim 54, Riley does not disclose, further comprising one or more biometric devices associated with at least one of a door to the cockpit area or a door to a storage compartment to restrict access to designated persons.

Seah discloses a monitoring and incident management system for an aircraft.

A biometric device, such as a fingerprint or retinal scanner is provided (col. 2, [0045]). The biometric subsystem is integrated into a double-door module of the cockpit, to determine whether a person trying to gain entry to the cockpit is authorized (col. 2, [0045], col. 3, [0050 and Fig. 10]. It would have been obvious to one having ordinary skill in the art at the time the invention was made to use the teachings of Seah to modify Riley's security system by using a biometric associated with a door to the cockpit area in order to deny entry to the cockpit to any person not authorized to be in the cockpit, as determined by the biometric device and to prevent a hijacker or terrorist from controlling the aircraft.

As to claim 55, seah further discloses, wherein the one or more biometric devices comprises a fingerprint reader (col. 2, [0045]).

As to claim 56, seah further discloses, further comprising a camera mounted on the cockpit area adapted for at least one of taking a retina read of designated persons in response to sensed motion or a photograph of designated persons (col.2, [0045]).

As to claim 57, seah further discloses, further comprising devices for transmitting the photograph to authorities outside of the aircraft (col. 2, [0045], col. 3, [0052] and [0057]).

14. Claims 24, 37 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Riley (U.S. Patent Application Publication 2003/0067379) as applied to claims 14, 27 and 40 above, and further in view of the combination of Osten et al. (U.S. Patent 5,719,950) and Ott (U.S. Patent 5,719,950).

As to claim 24, Riley discloses the use of a fingerprint scanner (biometric device) that has live finger detection capabilities to add a further measure of security (col. 3, [0039], last nine lines), the fingerprint scanner is mounted on the aircraft's control yoke 11 (control of aircraft) (Fig. 1, Yoke 11, fingerprint scanner 7) and send an alert signal to parties outside the aircraft such as air traffic control tower (authorities) upon detection of an unauthorized person (col. 3, [0041], col. 5, [0050]). Riley does disclose the specifics of the fingerprint scanner (biometric device) that has live finger detection capabilities and is silent about, wherein reading biometric information comprises reading pulses of the person when the person is grasping the control, the method further comprising alerting authorities outside of the aircraft when there is an unusual pulse reading from the person. However, using a pulse reader with the fingerprint scanner (biometric device) to detect a live finger in the context of access control is conventional and well known in the art as disclosed by Osten.

Oaten discloses a biometric system to assure that an individual seeking biometric authentication, recognition or access is actually present for authentication. For example, in a fingerprint scanner whether the finger is attached to a living human being or an electronic or photographic reconstruction of the fingerprint or dismemberment of the finger is used (col. 1, line 56-col. 2, line 10). One or more non-specific biometric parameters within a specific range (e.g., bone structure, EKG signals, pulse, and spectral characteristics of human tissue (col. 2, line 66-col. 3, line 13, lines 56-67) used in combination with one or more unique, inherently specific biometric parameters (e.g., fingerprints, handwriting and retinal configuration) (col. 2, lines 54-65) provides

extremely high precision protection against circumvention, and does not require time consuming and inordinate measurement for authentication for purposes such as access control to a secure function or fitness to perform a function (col. 3, lines 14-20).

Inherently specific and non-specific biometric parameters can be concurrently and non-invasively gathered for recognition, comparison, and authentication (col. 4, lines 43-46).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to use the teachings of Osten to modify Riley's security system by using a pulse reader in the fingerprint scanner to achieve a live finger detection capabilities (as disclosed by Riley) and concurrently gathering inherently specific (fingerprint, and retinal configuration) and non-specific (EKG signals, pulse, and spectral characteristics of human tissue) biometric parameters (as disclosed by Osten) in order to add a further measure of security and to provide extremely high precision protection against circumvention, and does not require time consuming and inordinate measurement for authentication for purposes such as access control to a secure function or fitness to perform a function. Osten does not disclose, the method further comprising alerting authorities outside of the aircraft when there is an unusual pulse reading from the person.

Ott discloses a system for automatic machine interrogation of individuals for identifying persons seeking access control (Abstract). The system detects and analyzes the characteristics of a human body part (col. 3, lines 13-20). The system determines the emotional state or tension of the person whose identity has been established. This is important where a person who is authorized to remove information from a computer

Art Unit: 2623

might be nervous because he is intending to do this for illegitimate reasons or under duress (col. 2, lines 6-15). It would have been obvious to one having ordinary skill in the art at the time the invention was made to use the teachings of Ott to modify the combined security system of Riley and Osten by determining the emotional state or tension of the person whose identity has been established in order to determine whether an authorized person accessing a machine is nervous because he is intending to do this for illegitimate reasons or under duress. Ott does not disclose an unusual pulse reading from the person. However, it is functionally inherent in a human being under emotional tension or nervous or under duress to have unusual pulse rate outside the normal pulse rate, and the combined system of Riley and Osten that uses pulse within a specific range for identification would be able to determine that the unusual pulse reading of a nervous or under duress person is outside the specific pulse range it is using.

As to claim 37, refer to claim 24 rejection.

As to claim 50, refer to claim 24 rejection.

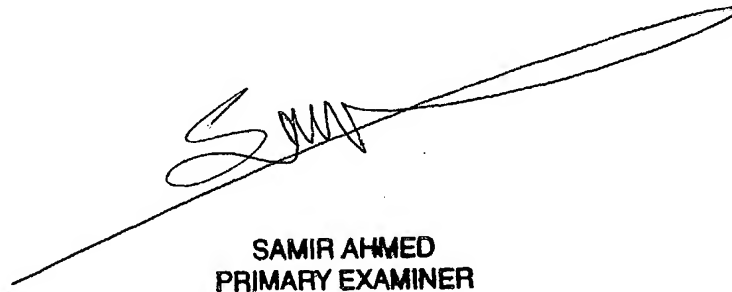
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samir A. Ahmed whose telephone number is 703-305-9870. The examiner can normally be reached on Mon-Fri 8:30am-6:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Amelia Au can be reached on 703-308-6604. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2623

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SA



**SAMIR AHMED  
PRIMARY EXAMINER**